CLAIMS

What is claimed is:

5   1.   In a computer network a method for detecting ARP spoofing, including:

receiving an ARP reply on a port of a network device;

generating a data packet, wherein the data packet includes information from the ARP reply, and an identification of the port on which the ARP reply was received;

storing information contained in the data packet in a database of an ARP

10   collector; and

analyzing the information in the database to determine when ARP spoofing occurs.

2.   The method of claim 1, wherein the generating the data packet, which

15   includes information from the ARP reply, includes encrypting the datapacket.

3.   The method of claim 1, wherein the information stored in the database includes a MAC address of a device which generated an ARP reply, and an IP address given as a source IP address in the ARP reply.

20

4.   The method of claim 1, wherein the information stored in the database includes a MAC address of a device which generated an ARP reply, and an IP address given as a source IP address in the ARP reply, and a time at which the ARP reply was received on the port.

25

5.   The method of claim 1, wherein the information stored in the database includes a MAC address of a device which generated the ARP reply, and an IP address given as a source IP address in the ARP reply, and a time at which the ARP reply was received on the port, and an identification of the port on which the ARP reply was received.

30

6.   The method of claim 1, wherein when it is determined that there is a spoofed ARP reply, blocking the port on which the spoofed ARP reply was received.

7.   The method of claim 1, wherein when it is determined that there is a spoofed
5   ARP reply, filtering a MAC address which generated the spoofed ARP reply at a port at which the spoofed ARP reply was received.

8.   The method of claim 1 further comprising:

transmitting the data packet to the ARP collector; and
10   generating an alert when an ARP spoofing condition occurs.

9.   In an ARP collector a method for detecting ARP spoofing, the method comprising:

receiving ATP packets from a first subnet of a computer network;
15   receiving ATP packets from a second subnet of the computer network;

storing information from the ATP packets from the first subnet in a database of the ARP collector;

storing information from the ATP packets from the second subnet in the database of the ARP collector; and
20   analyzing received ATP packets and information in ARP collector database to determine when a spoofed ARP reply has been received on a port of the computer network.

10.   The method of claim 9, further comprising:
25   blocking a port of the computer network which received a spoofed ARP reply.

11.   The method of claim 9, further comprising:

identifying a MAC address as a source for a spoofed ARP reply; and

filtering the identified MAC address at a port of the computer network which
30   received the spoofed ARP reply.

12.   The method of claim 9, wherein the ATP packets from the first subnet, and the ATP packets from the second subnet include ARP reply information received on ports of network devices in the respective subnets.

5

13.   The method of claim 9, wherein the ATP packets from the first subnet, and the ATP packets from the second subnet include ARP reply information received on ports of network devices in the respective subnets, and information in the ATP packets includes information identifying a port on which a particular ARP reply was received.

10

14.   The method of claim 9, wherein the storing information from the ATP packets from the first subnet, and the storing information from the ATP packets from the second subnet, includes:

storing ARP reply information indicating a MAC address which is identified

15   as a source of an ARP reply,

storing ARP reply information indicating an IP address which is identified as a source of an ARP reply; and

storing information indicating a port on which an ARP reply was received.

20   15.   A device for storing and analyzing ARP information to detect ARP spoofing, the device including:

an interface for receiving ATP packets, wherein the ATP packets include ARP reply information, including information identifying a port on a network device where an ARP reply was received;

25   a processor coupled to the interface, and programmed to analyze a first received ATP packet, and to identify a first MAC address which is identified as a source MAC address for a first ARP reply, and to identify a first IP address which is identified as a source IP address for the first ARP reply, and to identify a first port on which the first ARP reply was received;

30   a database coupled to the processor, and which stores information from the ATP packets, wherein for the first ATP packet received at the interface, the database

Atty Docket No.: FDRY-110

stores the first MAC address, the first IP address, and the port on which the first ARP

reply was received; and

wherein the processor is further operable to analyze information in the

database and information in a received ATP packet to identify when a spoofed ARP

5   reply has been transmitted by a host.

16.   The device of claim 15, further including a garbage collection timer module

which determines when ARP reply information is stale and should be cleared from the

database.

10

17.   The device of claim 15, wherein processor is further operable to generate an

alert when a spoofed ARP reply has been detected.

18.   The device of claim 15, wherein the processor is further operable, to identify a

15   port on which a spoofed ARP reply has been received and to generate a signal which causes

the port to be blocked in response to identifying the port on which the spoofed ARP reply has

been received.

19.   The device of claim 15, wherein the processor is further operable to identify a

20   port on which a first spoofed ARP reply has been received and to identify a MAC address of

an attacking host which generated the spoofed ARP reply, and in response to identifying the

port, and the MAC address of the attacking host, the processor generates a signal which

indicates that the MAC address should be MAC filtered at the port.

25